METHOD, COMPUTER-READABLE MEDIUM, AND NODE FOR DETECTING EXPLOITS BASED ON AN INBOUND SIGNATURE OF THE EXPLOIT AND AN OUTBOUND SIGNATURE IN RESPONSE THERETO

ABSTRACT OF THE INVENTION

A method of detecting an intrusion at a node of a network comprising reading a first packet received by the node, determining a first signature of the first packet, comparing the first signature with a signature file comprising a first machine-readable logic representative of a first packet signature, determining the first signature corresponds with the first machine readable logic, reading a second packet generated by the node in response to reception of the first packet, determining a second signature of the second packet, comparing the second signature with the signature file further comprising a second machine-readable logic representative of second packet signature, and determining the second signature corresponds with the second machine readable logic is provided. A computer-readable medium having stored thereon a set of instructions to be executed, the set of instructions, when executed by a processor, cause the processor to perform a computer method of reading a first packet, determining a first signature of the first packet, comparing the first signature with a first instruction set comprising a first set of machine readable logic representative of a first packet signature, determining the first signature corresponds with the first set of machine readable logic, reading a second packet, determining a second signature of the second packet, comparing the second signature with a second instruction set comprising a second set of machine readable logic representative of a second packet signature, and determining the second signature corresponds with the second set of machine readable logic is provided. A node of a network operable to detect an intrusion thereof is provided, the node comprising a central processing unit, a memory module for storing data in machine readable format for retrieval and execution by a central processing unit, and an operating system comprising a network stack comprising a protocol driver, a media access control driver and a network filter service provider bound to the protocol driver and the media access control driver, the network filter service provider operable to receive a first packet and to determine a

first signature of the first packet and compare the first signature with a first instruction set comprising a first set of machine readable logic representative of a first packet signature and to determine a correspondence with the first set of machine readable logic, the network filter service provider further operable to receive a second packet and to determine a second signature of the second packet and compare the second signature with a second instruction set comprising a second set of machine readable logic representative of a second packet signature and to determine a correspondence with the second set of machine readable logic, the processor operable to execute a directive comprised of machine readable instructions upon determination, by the network filter service provider, of a correspondence between the first signature and the first instruction set and correspondence between the second signature and the second instruction set. A method of detecting an intrusion at a node of a network comprising reading a packet by the node, determining a signature of the packet, comparing the signature with a signature file comprising a machine-readable logic representative of a packet signature, and determining the signature corresponds with the machine readable logic is provided.